UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,450	11/06/2001	Massimo DiPierro	089326-0101	8018

23644 7590 02/22/2006

BARNES & THORNBURG, LLP
P.O. BOX 2786
CHICAGO, IL 60690-2786

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,450	DIPIERRO, MASSIMO	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-26* is/are pending in the application.

4a) Of the above claim(s) *22,23,25 and 26* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20,21 and 24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 06 December 2005. Claims 20 and 21 have been amended. Claims 1-19 have been canceled. New claims 22-26 have been added. Claims 20-26 are currently pending in the present application.

Election/Restrictions

2. In the following analysis, reference is made to the following inventions:

I. Amended Claims 20 and 21, and new Claim 24, directed to methods for managing sensitive data including creating a file and performing an input-output operation on the file that decrypts, updates data, updates a digital signature, and re-encrypts, classified in class 713, subclass 176.

II. New Claims 22, 23, 25, and 26, directed to methods of developing an application (see Claim 23) and managing sensitive data using the developed application and associated functions, classified in class 717, subclass 174.

3. Newly submitted claims 22, 23, 25, and 26 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination

is separately usable. In the instant case, subcombination I has separate utility such as managing sensitive data by using functions other than those with the syntax required by invention II. See MPEP § 806.05(d).

Because these inventions are independent or distinct for the reasons given above and have acquired a separate status in the art in view of their different classification, restriction for examination purposes as indicated is proper.

Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 22, 23, 25, and 26 are withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Response to Arguments

4. Applicant's arguments with respect to claims 20, 21, and 24 have been considered but are moot in view of the new ground(s) of rejection.

Specification

5. Although the Applicant has corrected the errors in the specification that were specifically noted by the Examiner, the specification still appears to contain other errors. The objection is not withdrawn.

6. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, in paragraph 0038, lines 2-3, it appears that in the phrase "such and embodiment", "and" should be replaced with "an". In paragraph 0066, line 10, it appears that in the phrase "sets the sets the internal Header", one of the "sets the" should be deleted. Further, in paragraph 0142, lines 16-17, it appears that "is" should be deleted from the phrase "The executing code is successfully ascertains the corruption text file".

The Examiner again notes that the above is not to be considered an exhaustive list of errors in the specification. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is again requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, *Applied Cryptography*, in view of Brundrett et al, US Patent 6249866.

In reference to Claim 24, Schneier discloses a method that includes creating and encrypting a file containing sensitive data, and performing a file input-output operation on a proper subset of the file without needing to decrypt the entire file, where the operation includes decrypting a subset of the file when performing read and write operations, and encrypting a data subset to be written and writing the encrypted data (see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Schneier further discloses calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file. However, Schneier is silent as to whether the decryption operation is performed in a function local to a trusted application. Brundrett discloses an encrypting file system (EFS) and method where cryptographic functions are performed local to an application (see Figures 1 and 2, where the EFS Service 50 and Crypto API 58 interface with the application 30 at the user or application side; see also column 7, line 60-column 8, line

44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method suggested by Schneier by performing cryptographic functions local to the application, in order to provide a system and method in which encryption and decryption are transparent and data recovery is addressed, and which are flexible and extensible (see Brundrett, column 2, lines 7-25).

9. Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Borman et al, US Patent 5437026, and Brundrett.

In reference to Claim 20, Schneier discloses a method that includes storing sensitive data in an encrypted file, decrypting a subset of the file when performing read and write operations, and encrypting a data subset to be written and writing the encrypted data (see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Schneier further discloses calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file. However, Schneier does not explicitly disclose inputting the

subset from a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file and updating the file with the temporary copy when closing the file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24). Although Schneier and Borman disclose the above, Schneier and Borman are silent as to whether the decryption operation is performed in a function local to a trusted application. Brundrett discloses an encrypting file system (EFS) and method where cryptographic functions are performed local to an application (see Figures 1 and 2, where the EFS Service 50 and Crypto API 58 interface with the application 30 at the user or application side; see also column 7, line 60-column 8, line 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier and Borman by performing cryptographic functions local to the application, in order to provide a system and method in which encryption and decryption are transparent and data recovery is addressed, and which are flexible and extensible (see Brundrett, column 2, lines 7-25).

In reference to Claim 21, Schneier discloses a method that includes creating and encrypting a file containing sensitive data, and performing a file input-output operation on a proper subset of the file without needing to decrypt the entire file, where the operation includes decrypting a subset of the file when performing read and write operations, and encrypting a data subset to be written and writing the encrypted data

(see page 190, noting the first full paragraph where ECB mode is recommended for encryption of database records). Schneier further discloses calculating and storing a digital signature for a file (see page 30, section 2.4, "One-Way Hash Functions", where a hash can be created by pre-imaging a file and XORing strings of bits together). Therefore, it would have been obvious to combine the digital signature and encryption as taught by Schneier, in order to gain the integrity of digital signatures (see page 35) and the advantages of electronic codebook mode block encryption to allow blocks to be decrypted independently (see page 190). Further, it would have been obvious to one of ordinary skill in the art at the time the invention was made to update the digital signature after changing a file, so that the signature correctly reflects the contents of the file. However, Schneier does not explicitly disclose creating a temporary copy of the file. Borman discloses a method including creating a duplicate, temporary copy of a file and updating the file with the temporary copy when closing the file (see column 2, lines 12-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the creation of a temporary file copy, in order to allow for data recovery in the event of a system failure or abnormal termination (see Borman, column 1, lines 35-45; column 2, lines 14-24). Although Schneier and Borman disclose the above, Schneier and Borman are silent as to whether the decryption operation is performed in a function local to a trusted application. Brundrett discloses an encrypting file system (EFS) and method where cryptographic functions are performed local to an application (see Figures 1 and 2, where the EFS Service 50 and Crypto API 58 interface with the application 30 at the user or application side; see also column 7, line 60-column

8, line 44). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier and Borman by performing cryptographic functions local to the application, in order to provide a system and method in which encryption and decryption are transparent and data recovery is addressed, and which are flexible and extensible (see Brundrett, column 2, lines 7-25).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Blaze, US Patent 5721777, discloses a system that includes, *inter alia*, an encrypted file system.

b. Gupta, US Patent 6446109, discloses a system that includes tiers of access including a database tier, where a local application becomes trusted to access other tiers.

c. Gressel et al, US Patent 6749115, discloses a system that includes a security application in contact with a trusted application environment, where functions are performed local to the application.

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER